

This listing of claims will replace all prior versions, and listings, of claims in the application:

The Status of the Claims

1. (Currently amended) A method to provide network traffic support and physical security support comprising:

initializing a plurality of virtual machines, wherein each of the plurality of virtual machines operates like a complete physical machine that can run its own operating system;

initializing a virtual machine monitor (~~VMM~~) in a processor system during a pre-boot phase, wherein the virtual machine monitor is configured to manage the operation of the plurality of virtual machines;

identifying at least one of a network traffic intrusion event and a physical security intrusion event with the ~~VMM~~ virtual machine monitor,

wherein identifying the network traffic intrusion event includes:

detecting an incoming network packet;

determining whether the incoming network packet is attempting to access a restricted port;

discarding the network packet if the network packet is attempting to access a restricted port;

performing packet level virus scanning on the network packet to determine if the network packet is associated with a virus;

discarding the network packet if the network packet if the network packet is associated with a virus;

determining whether the incoming network packet is a denial of service attack;
discarding the incoming network packet if the incoming network packet is a
denial of service attack;
determining whether the incoming network packet is an alert standard format
packet; and
invoking a system manageability agent and performing a task if the incoming
network packet is an alert standard format packet; and
wherein identifying the physical security intrusion event includes:
detecting a physical intrusion;
determining whether a user has authorization to initiate the physical intrusion;
determining which components of the processor system are vulnerable to the
physical intrusion; and
disabling the components of the processor system that are vulnerable to the
physical intrusion if the user does not have authorization to initiate the physical intrusion.
~~implementing at least one of a network traffic support and a physical security support in~~
~~response to the at least one of the network traffic intrusion event and the physical security~~
~~intrusion event.~~

2. (Canceled)

3. (Currently amended) A method as defined in claim 1, wherein detecting a physical
intrusion identifying the at least one of the network traffic intrusion event and the physical
security intrusion event with the VMM comprises detecting opening of a chassis of the processor
system via a chassis intrusion switch.

4. (Canceled)

5. (Currently amended) A method as defined in claim 1, wherein ~~implementing the at least one of the network traffic support and the physical security support~~ disabling the components of the processor system that are vulnerable to the physical intrusion if the user does not have authorization to initiate the physical intrusion comprises disabling the processor system in response to identifying the physical security intrusion event.

6. (Canceled)

7. (Currently amended) A method as defined in claim 1, wherein the processor system is associated with at least one of a private internal network ~~and~~ or the Internet.

8. (Currently Amended) A machine readable medium storing instructions, which when executed, cause a machine to:

initialize a plurality of virtual machines, wherein each of the plurality of virtual machines operates like a complete physical machine that can run its own operating system;

initialize a virtual machine monitor (VMM) in a processor system during a pre-boot phase, wherein the virtual machine monitor is configured to manage the operation of the plurality of virtual machines;

identify at least one of a network traffic intrusion event and a physical security intrusion event with the ~~VMM~~ virtual machine monitor,

wherein the instructions cause the machine to identify the at least one of the network traffic intrusion event within the virtual machine monitor by:

detecting an incoming network packet;

determining whether the incoming network packet is attempting to access a restricted port;

discarding the network packet if the network packet is attempting to access a restricted port;

performing packet level virus scanning on the network packet to determine if the network packet is associated with a virus;

discarding the network packet if the network packet is associated with a virus;

determining whether the incoming network packet is a denial of service attack;

discarding the incoming network packet if the incoming network packet is a denial of service attack;

determining whether the incoming network packet is an alert standard format packet; and

invoking a system manageability agent and performing a task if the incoming network packet is an alert standard format packet; and

wherein the instructions cause the machine to identify the at least one of the physical security intrusion event within the virtual machine monitor by:

detecting a physical intrusion;

determining whether a user has authorization to initiate the physical intrusion;

determining which components of the processor system are vulnerable to the physical intrusion; and

disabling the components of the processor system that are vulnerable to the physical intrusion if the user does not have authorization to initiate the physical intrusion.

~~implement at least one of a network traffic support and a physical security support in response to the at least one of the network traffic intrusion event and the physical security intrusion event.~~

9. (Canceled)

10. (Currently amended) A machine readable medium as defined in claim 8, wherein the instructions cause the machine to identify the ~~at least one of the network traffic intrusion event and the physical security intrusion event~~ within the ~~VMM~~ virtual machine monitor by detecting opening of a chassis of the processor system via a chassis intrusion switch.

11. (Canceled)

12. (Canceled)

13. (Original) A machine readable medium as defined in claim 8, wherein the processor system is associated with at least one of a private internal network and the Internet.

14. (Original) A machine readable medium as defined in claim 8, wherein the machine readable medium comprises one of a programmable gate array, application specific integrated circuit, erasable programmable read only memory, read only memory, random access memory, magnetic media, and optical media.

15. (Currently amended) An apparatus to provide network traffic support and physical security support comprising:

a data structure configured to store firmware of a processor system; ~~and~~

a plurality of virtual machines initialized from the firmware during a pre-boot phase to operate like a complete physical machine that can run its own operating system;

a virtual machine monitor initialized from the firmware during a pre-boot phase to identify at least one of a network traffic intrusion event and a physical security intrusion event,

wherein identifying the network traffic intrusion event includes:

detecting an incoming network packet;

determining whether the incoming network packet is attempting to access a restricted port;

discarding the network packet if the network packet is attempting to access a restricted port;

performing packet level virus scanning on the network packet to determine if the network packet is associated with a virus;

discarding the network packet if the network packet if the network packet is associated with a virus;

determining whether the incoming network packet is a denial of service attack;

discarding the incoming network packet if the incoming network packet is a denial of service attack;

determining whether the incoming network packet is an alert standard format packet; and

invoking a system manageability agent and performing a task if the incoming network packet is an alert standard format packet; and
wherein identifying the physical security intrusion event includes:
detecting a physical intrusion;
determining whether a user has authorization to initiate the physical intrusion;
determining which components of the processor system are vulnerable to the physical intrusion; and
disabling the components of the processor system that are vulnerable to the physical intrusion if the user does not have authorization to initiate the physical intrusion.
~~and to implement at least one of a network traffic support and a physical security support in response to detecting the at least one of the network traffic intrusion event and the physical security intrusion event.~~

16. (Canceled)

17. (Original) An apparatus as defined in claim 15, wherein the physical security intrusion event comprises opening a chassis of the processor system.

Claims 18-20 (Canceled)

21. (Original) An apparatus as defined in claim 15, wherein the data structure comprises a flash memory.

Claims 22-32 (Canceled)